Policies and Procedures
POLICY: Breach Notification and Mitigation Policy
Policy #21
Effective Date: November 7, 2013

Purpose: HIPAA, HITECH, the Illinois Personal Information Protection Act ("PIPA"), and other Applicable Law require notice of a Breach. Should there be a Breach of Protected Health Information utilizing ILHIE technology or infrastructure, Breach notification and mitigation obligations may apply to both a Participant(s) and the ILHIE Authority, in its Business Associate capacity to Participants.

This Policy and Procedure establishes a Breach notification and mitigation protocol for Participants and the ILHIE Authority. It applies only to those privacy and security incidents which would qualify as a Breach under HIPAA, HITECH or other Applicable Law and which utilize ILHIE technology or infrastructure or which allow unauthorized access to ILHIE technology, ILHIE infrastructure or Protected Health Information through the ILHIE. The obligations contained herein comply with and supplement those obligations contained in HIPAA, HITECH or other Applicable Law. This policy shall be incorporated by reference into all existing and future Data Sharing Agreements entered into by and between Participants and the ILHIE Authority.

Policy: A Participant shall, promptly upon discovery of a Breach (whether a Breach of the ILHIE, or a Breach by the Participant, an Other Participant or the ILHIE Authority) report the Breach to the ILHIE Authority and the Affected Participants in accordance with this Policy and Procedure.

1.0 **Participant Breach**. A Breaching Participant shall, in accordance with its own policies, promptly investigate any and all Breaches. The Breaching Participant shall inform the ILHIE Authority and, in those cases where the Affected Participants can be identified, inform the Affected Participants of a Breach in accordance with the procedures set forth herein.

1.1 The Breaching Participant shall be responsible for notifying Individuals, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with those provided by any Affected Participant. An Affected Participant may also notify Individuals with whom the Affected Participant has or had a relationship and whose Protected Health Information was compromised by the Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that Affected Participants providing such notification shall use reasonable efforts to advise and coordinate any notice with the Breaching Participant, as well as the ILHIE Authority.

1.2 The Breaching Participant shall be responsible for mitigating the Breach. The ILHIE Authority shall have the right to participate in the investigation and to know the results and remedial action taken, if any, except that the ILHIE Authority need not be notified of specific workforce disciplinary actions and may not participate in any action or investigation by a Participant that would result in the loss of any applicable attorney-client privilege or work product protections. This Policy and Procedure shall not be interpreted in a way that would require a Participant to disclose Protected Health Information to the ILHIE Authority if such disclosure is not permitted under HIPAA, HITECH, or other Applicable Law.

2.0 **ILHIE Breach.** The ILHIE Authority shall, in accordance with the procedures set forth herein, promptly upon discovery of any ILHIE Breach, report such ILHIE Breach to the Breaching Participant, as well as to the Affected Participants. The ILHIE Authority shall promptly investigate any ILHIE Breach, mitigate the ILHIE Breach, and cooperate with the Breaching Participant and all Affected Participants with respect to any mitigation, reporting or other obligations that the Breaching Participant, the Affected Participants or both may have. Each Breaching or Affected Participant shall be responsible for notifying Individuals to the extent required under HIPAA, HITECH, or other Applicable Law. The ILHIE Authority shall not give such notice unless and to the extent that a Participant has delegated to the ILHIE Authority the obligation to provide notice on behalf of that Participant. Notwithstanding the foregoing, the ILHIE Authority shall give any notice that it is required to provide under applicable law.

3.0 **Role of ILHIE Authority.** Upon Breaching Participant request, the ILHIE Authority shall assist the Breaching Participant in identifying Affected Participants. Where multiple Participants are Breaching Participants or Affected Participants, upon the request of one or more Participants, the ILHIE Authority may coordinate communication and activities between those Participants, but nothing set forth in this Policy and Procedure shall require any Participant to delay its own investigation, reporting, or other activities that it deems necessary or appropriate to comply with Applicable Law or to assure the ongoing privacy and security of Protected Health Information. The ILHIE Authority shall not be responsible for making determinations as to which Participant is responsible for a Breach.

3.1 For all Breaches, an investigation of a Breach and all actions taken with respect to the Breach, shall be documented and provided to the ILHIE Authority by the Breaching Participant. The ILHIE Authority may use this information for education, policy, and the development of safeguards.

3.2 The ILHIE Authority shall prepare an annual report for Participants identifying Breaches which occurred within the previous year which utilized ILHIE technology or infrastructure, or which allowed unauthorized access to ILHIE technology, ILHIE infrastructure or Protected Health Information through the ILHIE. Nothing, however, precludes the ILHIE Authority from notifying Participants more frequently if the ILHIE Authority determines that doing so will be beneficial to ILHIE operations. The ILHIE Authority shall not disseminate or publish Protected Health Information. The ILHIE Authority may

disseminate or publish de-identified data to provide examples of Breaches for education, policy, and the development of safeguards.

4.0 **Cooperation.** Participants shall appoint an individual to be contacted in the event of a Breach and shall notify the ILHIE Authority of this person and their contact information, including any changes thereto.

4.1 A Participant shall, promptly upon discovery of any Breach (whether a Breach of the ILHIE, or a Breach by the Participant, an Other Participant, or the ILHIE Authority) report by email the Breach to the ILHIE Authority and the Affected Participants. Participants are not responsible for monitoring the ILHIE or Other Participants for Breaches. Where a Participant reports an incident in good faith, the Participant will not be liable if the incident reported is subsequently determined not to be a Breach.

4.2 Participants shall cooperate in any good faith investigations conducted by the ILHIE Authority. Participants and the ILHIE Authority shall cooperate in any good faith investigations conducted by an Other Participant. In addition, a Participant shall cooperate with the legally required notification and mitigation activities of Other Participants or the ILHIE Authority.

5.0 **Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

5.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

6.0 **Sanctions.** The ILHIE Authority may immediately suspend or revoke an Authorized User's ILHIE access for cause in accordance with the Sanction Policy (Policy #15) and the Data Sharing Agreement.

Participant Breach Procedures

1.0 *Investigation*. A Breaching Participant shall, in accordance with its own policies, promptly investigate suspected or actual reported Breaches.

2.0 *Notifying the ILHIE Authority and Affected Participants ("Informational Notification")*. A Breaching Participant shall notify the ILHIE PCO and, in those cases where the Affected Participants can be identified, the Affected Participants of a Breach. The ILHIE Authority shall make Participant contact information available to all Participants to facilitate informational notification. No notification is required regarding the ongoing existence, occurrence or attempt of unsuccessful security incidents, including pings and other broadcast attacks on a Participant's firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized acquisition, access, use, or disclosure of Protected Health Information.

2.1 Informational Notification shall be made promptly, but in no event more than five (5) business days from discovery of a Breach. Notification shall be made irrespective of whether the Breaching Participant's investigation is complete.

2.2 Informational Notification shall be done (i) via email or (ii) via phone conference with the ILHIE PCO and Affected Participants, provided that notice by email is subsequently provided to all Affected Participants and the ILHIE PCO.

2.3 Informational Notification shall include sufficient information so that the ILHIE PCO, if requested by a Participant, can assist the Participant in its investigation and mitigation efforts. Informational Notification should include, but need not be limited to, the items set forth on Exhibit 1 to the extent that the Breaching Participant has knowledge of such items.

2.4 Upon determination that a previously reported Breach is not a Breach, the Participant that reported the Breach shall send an updated status to the ILHIE Authority and Affected Participants.

3.0 *Notification Required by Law ("Legal Notification").* Except as provided in the ILHIE Authority Breach Procedures Section, the Breaching Participant shall, at its expense, be responsible for notifying Individuals, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with the Affected Participant(s). An Affected Participant may also notify Individuals with whom the Affected Participant has or has had a relationship and whose Protected Health Information was compromised by the Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other Individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that Affected Participants providing such notice shall use reasonable efforts to advise and coordinate any notice with the Breaching Participant and the ILHIE Authority.

4.0 *Mitigation and Remediation.* The Breaching Participant shall take reasonable steps to pursue, address, and mitigate any Breach which has resulted from its acts or omissions, which may include a request to any party who improperly received such information to return and/or destroy the impermissibly disclosed information.

4.1 The Breaching Participant shall assume mitigation costs incurred by itself and the ILHIE Authority and Affected Participants, which were caused by the Breach of the Breaching Participant. Mitigation costs shall not include special, consequential, indirect, exemplary, or punitive damages as further described in the Data Sharing Agreement. The Breaching Participant(s), the ILHIE Authority, and any Affected Participant(s), shall coordinate mitigation efforts to minimize duplication of efforts. Disputes with respect to this Section shall be resolved in accordance with any dispute resolutions mechanism set forth in the Data Sharing Agreement.

5.0 *Reporting Requirements.* The investigation of a Breach and all actions taken with respect to the Breach shall be documented, and the documentation shall be provided by the Breaching Participant to the ILHIE Authority within thirty (30) days of the provision of Legal Notification to Individuals. The documentation should include, but need not be limited to, the items set forth on Exhibit 2, to the extent that the Breaching Participant has knowledge of such items. The ILHIE Authority need not be notified of specific workforce disciplinary actions and may not participate in any action or investigation by a Participant that would result in the loss of any applicable attorney-client privilege or work product protections. This Policy and Procedure shall not be interpreted to require any Participant to disclose any Protected Health Information to the ILHIE Authority if such a disclosure would not be permitted under HIPAA, HITECH, or other Applicable Law.

6.0 *Role of ILHIE Authority.* If multiple Participants cannot agree on which is the Breaching Participant, on the request of one or more Participants, then the ILHIE Authority may facilitate the resolution of the matter.

6.1 The ILHIE Authority shall facilitate conference calls and other mechanisms to help Participants coordinate their responses and communications regarding Breaches to ensure that all such Participants are aware of mitigation efforts and costs, and to ensure that the Breach is generally described in the same way in press releases and government filings.

6.2 The ILHIE Authority shall develop template documents to facilitate communication of Breaches to Individuals, the Department of Health and Human Services, and the media, as well as other Individuals or entities requiring notification pursuant to HIPAA, HITECH, or other Applicable Law. Use of such templates is not required.

6.3 The ILHIE Authority may suspend or revoke an Authorized User in accordance with the Sanction Policy (Policy #15) and the relevant Participant's Data Sharing Agreement.

6.4 All Protected Health Information that the ILHIE Authority receives, or to which it has access in connection with any Breach, shall be subject to the requirements of its Business Associate Agreement(s) with Participant(s) and to HIPAA, HITECH, or other Applicable Law.

6.5 The ILHIE Authority shall take all action necessary to prevent any Protected Health Information that it receives in connection with a Breach from being subject to disclosure or release under the Illinois Freedom of Information Act (5 ILCS 140/1 *et seq*.) or similar federal or Illinois law or regulation requiring disclosure of government records or information.

ILHIE Breach Procedures

1.0 *Investigation.* The ILHIE Authority shall, in accordance with its own policies, promptly investigate actual or suspected ILHIE Breaches.

2.0 *Informational Notification*. The ILHIE Authority shall inform the Breaching Participant, as well as Affected Participants, of an ILHIE Breach. No notification is required regarding the ongoing existence and occurrence or attempts of unsuccessful security incidents, including pings and other broadcast attacks on the ILHIE's firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized acquisition, access, use, or disclosure of Protected Health Information.

2.1 Informational Notification shall be made as soon as possible, but in no event more than five (5) business days from discovery of the ILHIE Breach. Notification shall be made irrespective of whether the ILHIE Authority's investigation is complete.

2.2 Informational Notification shall be made (i) via email or (ii) via phone conference with the ILHIE PCO, Breaching Participant, and Affected Participants, provided that an email notice is subsequently provided to all parties.

2.2 Informational Notification shall include sufficient information so that each Participant that receives notification can conduct its own investigation and mitigation efforts. Informational Notification should include, but need not be limited to, the items set forth on Exhibit 1, to the extent that the ILHIE Authority has knowledge of such items.

2.3 Upon a determination that a previously reported ILHIE Breach is not Breach, the ILHIE Authority shall send an updated status to any Breaching Participants and Affected Participants.

3.0 *Notification Required by Law ("Legal Notification")*. A Breaching Participant shall be responsible for notifying Individuals, the Department of Health and Human Services, and, if necessary, the media, as well as other entities, if such notice required under HIPAA, HITECH, or other Applicable Law, about an ILHIE Breach; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with any Affected Participant. An Affected Participant may also notify Individuals with whom the Affected Participant has or had a relationship and whose Protected Health Information was compromised by the ILHIE Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other individuals or entities, if such notice is required under HIPAA, HITECH, or other Applicable Law; provided, however, that Affected Participants providing such notification shall use reasonable efforts to coordinate any notice with and advise any Breaching Participant and the ILHIE Authority. The Breaching and Affected Participants may delegate to the ILHIE Authority notification of Individuals about an ILHIE Breach on the Breaching Participant's or Affected Participant's behalf. The ILHIE Authority shall pay for the costs of Individual notification pertaining to an ILHIE Breach incurred by either the Breaching Participant, the Affected Participant, or by the ILHIE Authority on behalf of the Breaching Participant or Affected Participant.

4.0 *Mitigation and Remediation*. ILHIE Authority shall take reasonable steps to pursue, address, and mitigate any ILHIE Breach, which may include a request to the party

who improperly received such information to return or destroy the impermissibly disclosed information.

4.1 In accordance with the terms of the Data Sharing Agreement and Applicable Law, the ILHIE Authority shall assume mitigation costs incurred by itself, Breaching Participants and Affected Participants and which were caused by an ILHIE Breach. Mitigation costs shall not include special, consequential, indirect, exemplary, or punitive damages as further described in the Data Sharing Agreement. The ILHIE Authority, Breaching Participants and any Affected Participants shall coordinate mitigation efforts to minimize duplication of efforts. Disputes with respect to this Section shall be resolved in accordance with the dispute resolution mechanism set forth in the applicable Data Sharing Agreement.

5.0 *Reporting*. An investigation of an ILHIE Breach and all actions taken with respect to the ILHIE Breach by the ILHIE Authority shall be documented, and the ILHIE Authority shall provide such documentation to any Breaching Participant and Affected Participants within thirty (30) days of the provision of Legal Notification to Individuals. Documentation should include, but need not be limited to, the items set forth in Exhibit 2, to the extent that the ILHIE Authority has knowledge of such items.

6.0 *Coordination between Participants*. ILHIE Authority shall perform the role set forth in the Participant Breach Procedures Section of this Policy with respect to ILHIE Breaches.

Associated Policies and References

Data Sharing Agreement
45 C.F.R §164.400 et seq.
Public Law 111-005
Personal Information Protection Act, 815 ILCS 530/

Exhibits

EXHIBIT 1: INFORMATIONAL NOTIFICATION REQUIREMENTS

To the extent known, the following information shall be submitted to the ILHIE Authority as well as other Affected Participants upon the discovery of a Breach or suspected Breach.

1. Date of Breach or suspected Breach.

2. Date of discovery.

3. Description of Breach or suspected Breach. Please be specific and include the number of Individuals affected.

4. Description of Protected Health Information acquired, accessed, used, or disclosed. Please be specific as to the type of information.

5. Whether or not the following Protected Health Information was included in the unauthorized acquisition, access, use, or disclosure as well as explanatory details:

    - HIV/AIDS information including whether an HIV test was administered
    - genetic testing or counseling information
    - alcohol or substance abuse information
    - mental health and developmental disability information

6. Whether or not the following information was included (in whole or in part) in the unauthorized acquisition, access, use, or disclosure as well as explanatory details:
    - Social security number
    - Driver's license or State ID number
    - Account number, or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account

7. Recipient of unauthorized acquisition, access, use, or disclosure (include full identification, address, email, and phone number).

8. Description of any actions taken thus far with respect to investigation and mitigation efforts.

EXHIBIT 2: BREACH REPORT REQUIREMENTS

To the extent known, the following information shall be submitted to the ILHIE Authority as well as other Affected Participants within thirty (30) days of the provision of Legal Notification to Individuals.

1. Date of Breach.

2. Date of discovery.

3. Description of Breach. Please be specific and include the number of Individuals affected.

4. Description of Protected Health Information acquired, accessed, used, or disclosed. Please be specific as to the type of information.

5. Whether or not the following Protected Health Information was included in the unauthorized acquisition, access, use, or disclosure as well as explanatory details:

    - HIV/AIDS information including whether an HIV test was administered
    - genetic testing or counseling information
    - alcohol or substance abuse information
    - mental health and developmental disability information

6. Whether or not the following information was included (in full or in part) in the unauthorized use or disclosure as well as explanatory details:
    - Social security number
    - Driver's license or State ID number
    - Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account

7. Recipient of unauthorized acquisition, access, use, or disclosure (include full identification, address, email, and phone number).

8. Description of investigation.

9. Description of all applicable mitigation actions, including, but not limited to:

    - Retrieval of Protected Health Information
    - Whether or not disciplinary action was taken. NOTE: Specific details are not required

- Technical modifications
- Administrative modifications (e.g., adoption or modification of policies, workflow processes, etc.)
- Physician modifications
- Retraining
- Credit monitoring provided to Individuals
- Other

10. Date notification provided to Individuals.

11. Date notification provided to the Department of Health and Human Services.

12. Date notification provided in media (if required).

Definitions
Affected Participant
Authorized User
Breach(es)
Breaching Participant
Department of Health and Human Services
HIE
HIPAA
HITECH
ILHIE
ILHIE Authority
ILHIE Breach
ILHIE PCO
Informational Notification
Legal Notification
Participant
System